WHAT IS CLAIMED IS:

1. An extended key preparing apparatus wherein extended keys are prepared in common key cryptosystem from a cryptographic key input, comprising:

a dividing unit which divides binary digit string of said cryptographic key into a plurality of elements each composed of a predetermined bit length;

an intermediate data preparing unit which prepares a plurality of intermediate data by applying a plurality of times an operation wherein a predetermined constant is used to the respective elements divided by said dividing unit;

a selecting unit which selects a plurality of intermediate data corresponding to the number of stages of extended keys from the plurality of the intermediate data prepared by said intermediate data preparing unit; and

an extended key preparing unit which prepares the extended keys corresponding to said number of stages by converting irreversibly the plurality of the intermediate data selected by said selecting unit.

2. An extended key preparing apparatus according to claim 1 wherein said intermediate data preparing unit is provided with a nonlinear type operating unit for effecting nonlinear

type operation with respect to the respective elements divided by said dividing unit.

3. An extended key preparing apparatus according to claim 2 wherein said nonlinear type operating unit performs nonlinear type operation in such a manner that when said cryptographic key is divided into eight elements of 32 bits by said dividing unit, said nonlinear type operating unit separates said elements into 6, 5, 5, 5, 5, and 6 bits to transpose the same into other data, respectively, and the data after transposition are subjected to nonlinear type operation by the use of a determinant.

4. An extended key preparing apparatus according to claim 2 wherein said intermediate data preparing unit is provided with:

an addition unit which adds a constant to an odd number-th element that has been subjected to nonlinear type operation;

a multiplication unit which multiplies an even number-th element which has been subjected to nonlinear type operation by said constant; and

an exclusive OR operating unit which effects exclusive OR operation of said odd number-th element to which has been added the constant and said even number-th element which is succeeding to said odd number-th and to which has been multiplied by said constant.

5. An extended key preparing apparatus according to claim 4, comprising further a unit for preparing intermediate data by subjecting nonlinear type operation to the result of said exclusive OR operation of said odd number-th element and said even number-th element which is succeeding to said odd number-th.

6. An extended key preparing apparatus according to claim 5 wherein said addition unit and said multiplication unit repeat the plurality of times additions and multiplications by the use of the number i of different constants, respectively, to prepare the number i of data in every elements; said exclusive OR operating unit repeat i times operations for acquiring exclusive OR of the odd number-th element and the even number-th element which have been operated by the use of the same constants; and said preparing unit prepare the number i of intermediate data in every elements.

7. An extended key preparing apparatus according to claim 6 wherein said selecting unit selects one intermediate data corresponding to said number of stages of an extended key among the number i of intermediate data contained in the

respective elements which have been prepared by said intermediate data preparing unit.

8. An extended key preparing apparatus according to claim 1 wherein said extended key preparing unit is provided with:

a rearrangement unit which rearranges a plurality of intermediate data selected by said selecting unit; and

an irreversible conversion unit which converts irreversibly the plurality of intermediate data that have been rearranged by said rearrangement unit.

9. An extended key preparing apparatus according to claim 8 wherein when intermediate data are rearranged in an order of elements X, Y, Z, and W by said rearrangement unit, said irreversible converting unit prepares a first data by adding the element Y to a data obtained by shifting cyclically the element X leftwards by 1 bit; prepares a second data determined by sifting cyclically the data leftwards by further 1 bit, which data has been obtained by subtracting the element W from a data obtained by shifting cyclically said element Z leftwards by 1 bit; and operates exclusive OR of said first data and said second data.

10. An extended key preparing apparatus according to claim 1 wherein said dividing unit divides a cryptographic key of 128 bits, 192 bits, or 256 bits into eight elements of 32 bits.

11. An extended key preparing method wherein extended keys are prepared in common key cryptosystem from a cryptographic key input, comprising the steps of,

dividing binary digit string of said cryptographic key into a plurality of elements each composed of a predetermined bit length;

preparing a plurality of intermediate data by applying the plurality of times an operation wherein a predetermined constant is used to the respective elements divided by said dividing step;

selecting a plurality of intermediate data corresponding to the number of stages of extended keys from the plurality of the intermediate data prepared by said intermediate data preparing step; and

preparing the extended keys corresponding to said number of stages by converting irreversibly the plurality of the intermediate data selected by said selecting step.

12. An extended key preparing method according to claim 11 wherein said intermediate data preparing step involves a nonlinear type operating step for effecting nonlinear type operation with respect to the respective elements divided by said dividing step.

13. An extended key preparing method according to claim 12 wherein said nonlinear type operating step performs nonlinear type operation in such a manner that when said cryptographic key is divided into eight elements of 32 bits by said dividing step, said nonlinear type operating step separates said elements into 6, 5, 5, 5, 5, and 6 bits to transpose the same into other data, respectively, and the data after transposition are subjected to nonlinear type operation by the use of a determinant.

14. An extended key preparing method according to claim 12 wherein said intermediate data preparing step involves:

an addition step for adding a constant to an odd number-th element that has been subjected to nonlinear type operation;

a multiplication step for multiplying an even number-th element which has been subjected to nonlinear type operation by said constant; and

an exclusive OR operating step for effecting exclusive

OR operation of said odd number-th element to which has been added the constant and said even number-th element which is succeeding to said odd number-th and to which has been multiplied by said constant.

15. An extended key preparing method according to claim 14, comprising further a step for preparing intermediate data by subjecting nonlinear type operation to the result of said exclusive OR operation of said odd number-th element and said even number-th element which is succeeding to said odd number-th.

16. An extended key preparing method according to claim 15 wherein said addition step and said multiplication step repeat the plurality of times additions and multiplications by the use of the number i of different constants, respectively, to prepare the number i of data in every elements; said exclusive OR operating step repeat i times operations for acquiring exclusive OR of the odd number-th element and the even number-th element which have been operated by the use of the same constants; and said preparing step prepare the number i of intermediate data in every elements.

17. An extended key preparing method according to claim 16 wherein said selecting step selects one intermediate data corresponding to said number of stages of an extended key among the number i of intermediate data contained in the respective elements which have been prepared by said intermediate data preparing step.

18. An extended key preparing method according to claim 11 wherein said extended key preparing step involves:

a rearrangement step for rearranging a plurality of intermediate data selected by said selecting step; and

an irreversible conversion step for converting irreversibly the plurality of intermediate data that have been rearranged by said rearrangement step.

19. An extended key preparing method according to claim 18 wherein when intermediate data are rearranged in an order of elements X, Y, Z, and W by said rearrangement step, said irreversible converting step prepares a first data by adding the element Y to a data obtained by shifting cyclically the element X leftwards by 1 bit; prepares a second data determined by sifting cyclically the data leftwards by further 1 bit, which data has been obtained by subtracting the element W from a data obtained by shifting cyclically said element Z leftwards by 1 bit; and operates exclusive OR of said first

data and said second data.

20. An extended key preparing method according to claim 11 wherein said dividing step divides a cryptographic key of 128 bits, 192 bits, or 256 bits into eight elements of 32 bits.

21. A computer readable recording medium wherein an extended key preparing program in which extended keys are prepared in common key cryptosystem from a cryptographic key input is to be recorded, comprising:

recording the program containing a dividing step for dividing binary digit string of said cryptographic key into a plurality of elements each composed of a predetermined bit length;

an intermediate data preparing step for preparing a plurality of intermediate data by applying the plurality of times an operation wherein a predetermined constant is used to the respective elements divided by said dividing step;

a selecting step for selecting a plurality of intermediate data corresponding to the number of stages of extended keys from the plurality of the intermediate data prepared by said intermediate data preparing step; and an extended key preparing step for preparing the extended keys corresponding to said number of stages by converting irreversibly the plurality of the intermediate data selected by said selecting step.

22. An extended key preparing program in which extended keys are prepared in common key cryptosystem from a cryptographic key input, comprising:

recording the program containing a dividing step for dividing binary digit string of said cryptographic key into a plurality of elements each composed of a predetermined bit length;

an intermediate data preparing step for preparing a plurality of intermediate data by applying the plurality of times an operation wherein a predetermined constant is used to the respective elements divided by said dividing step;

a selecting step for selecting a plurality of intermediate data corresponding to the number of stages of extended keys from the plurality of the intermediate data prepared by said intermediate data preparing step; and

an extended key preparing step for preparing the extended keys corresponding to said number of stages by converting irreversibly the plurality of the intermediate data selected by said selecting step.